UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,342	04/12/2001	David John Craft	AUS920010088US1	3785

50675 7590 03/13/2008

IBM CORP. (CLG)
c/o CARDINAL LAW GROUP
1603 ORRINGTON AVENUE
SUITE 2000
EVANSTON, IL 60201

EXAMINER	
PICH, PONNOREAY	
ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
03/13/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/833,342	CRAFT ET AL.	
	Examiner	Art Unit	
	PONNOREAY PICH	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *10-12,16-20,23-26,29-33 and 37-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *10-12,16-20,23-26,29-33 and 37-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 10-12, 16-20, 23-26, 29-33, and 37-39 are pending.

Response to Amendment and Arguments

Applicant's amendments were fully considered. Applicant's arguments directed at the amended claims were fully considered, but are moot in view of new rejections made below in response to the amendments.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Note that it is determined that a person of ordinary skill in the art with respect to the current application has at least a BS in Computer Science/Engineering (or someone with equivalent industry experience) and is familiar with basic cryptographic concepts such as asymmetric key systems.

Claims 10 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (US 5,787,172) in view of Aoki (US 6,745,530) in further view of Epstein et al (US 6,694,025) in further view of Rose (US 5,708,709).

Claims 10 and 16:

As per claim 10, Arnold discloses the following limitations were well known in the art at the time applicant's invention was made:

1. Generating a client message at the client (col 2, lines 9-24).
2. Retrieving an embedded server public key from a memory structure in an article of manufacture (col 2, lines 9-24).
3. Encrypting the client message with the embedded server public key (col 2, lines 9-24).
4. Sending the client message to the server (col 2, lines 9-24).

Arnold does not explicitly disclose that in the prior art he discusses, the memory structure is read-only memory. Arnold also does not explicitly disclose the article of manufacture is in the client, the read-only memory structure having an embedded client private key, the embedded server public key and the embedded client private key not being related by a public/private key pair relationship, the embedded client private key being associated with a client public key generated and stored exclusively outside the client.

However, Arnold discloses read-only memory being used to store keys (col 4, lines 14-17). At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify the prior art teachings disclosed by Arnold so that the memory structure used to store keys was read-only memory structure. One skilled would have been motivated to do so because one skilled would appreciate that utilizing read-only memory to store keys would allow key information to be retained even if the device containing the memory were to lose power. One skilled would also be motivated to do so because use of read-only memory to store the

keys prevents tampering with information stored in the memory, thus providing better security (Arnold: col 4, lines 36-40).

Further, Aoki discloses the article of manufacture is in the client, the memory structure having an embedded client private key, the embedded server public key and the embedded client key not being related by a public private key pair relationship, the embedded client private key being associated with a client public key stored exclusively outside the client (Fig 1, item 200). Note that in the figure cited, the client has stored in memory, the client's private key (i.e. individual private key) and a server's public key, but no client public key. As the client does not store the client's public key, the client's public key is stored exclusively outside the client. The private key of the client and the server's public key are not related by a public/private key pair relationship as they do not have an inverse relationship with one-another, i.e. plaintext encrypted by one cannot be decrypted by the other.

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify the client/server system disclosed by Aoki to use the secure communication techniques taught by Arnold (what he reveals was known in the prior art as well as what his own invention uses). One skilled would have been motivated to do so because it would allow Aoki's network system to establish a private and secure link between the clients and server of his invention for secure communication (Arnold: col 2, lines 23-24 and 43-44).

Aoki also does not explicitly disclose that the client's public key was generated exclusively outside the client. However, Epstein discloses that it was well known in the prior art to generate public/private key pairs exclusively outside the client, i.e. via a key generation server (col 2, lines 31-39; col 3, line 62-col 4, line 3; and col 4, lines 11-24). At the time applicant's

invention was made, it would have been obvious to one of ordinary skill in the art to further modify the combination invention of Arnold and Aoki such that the client's public key was generated exclusively outside the client. One skilled would have been motivated to do so because as discussed by Epstein, the generation of a public/private key pair requires significant computational resources and generating the key pair outside the client would avoid the cost and loss of control that may result by enabling each user/client in a network environment to create the key pair (col 2, lines 31-39).

Arnold, Aoki, and Epstein do not explicitly disclose receiving a server message including application code from the server at the client in response to the client message, the application code having a first portion encrypted with a server private key and a second portion; and authenticating the first portion of the application code with the embedded server public key.

However, Rose discloses receiving a server message including application code from the server at the client in response to the client message, the application code having a first portion encrypted with a server private key and a second portion (Fig 4; col 3, lines 50-53; and col 5, lines 44-47). Figure 4 shows the format of an application code that is transmitted to the client in response to the client's request for the code. As seen in the Figure, the application code is composed of several portions. The first portion, item 182, is encrypted using the server's private key and the rest is considered the claimed second portion. Rose further discloses authenticating the first portion of the application code with the server public key (col 8, lines 15-31 and col 10, lines 4-29). Since the first portion of the application code seen in Figure 4 is encrypted using the server's private key, the server's public key is used to decrypt portion 182.

The control information contained therein is authenticated as discussed in cited columns 8 and 10.

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Arnold, Aoki, and Epstein's combination invention using Rose's teachings such that the client's message is used to request an application code from a server and in response to the request, an application code in the format recited in claim 10 is sent back to the client and the sent application code was authenticated using the embedded server public key. Arnold's prior art, Arnold, Aoki, Epstein, and Rose are all concerned with secure communication between a client and a server using asymmetric cryptographic techniques, thus the incorporation of Rose's teachings within the combination invention of Arnold, Aoki, and Epstein in the manner discussed would be nothing more than use of a known technique to improve similar devices (methods or products) in the same way. As per KSR v. Teleflex 550 U.S. ___, 127 S. Ct. 1727 (2007), this makes the invention as claimed obvious and unpatentable.

Claim 16 is directed towards a computer program product comprising instructions for implementing the method of claim 10, thus is rejected for much the same reasons as claim 10.

Claims 11 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (US 5,787,172) in view of Aoki (US 6,745,530) in further view of Epstein et al (US 6,694,025) in further view of Rose (US 5,708,709) and in further view of Sandhu et al (US 2002,0078344).

Claims 11 and 17:

As per claims 11 and 17, the combination of Arnold and Aoki discloses embedded client private key in a memory structure in an article of manufacture in the client (Aoki: Fig 1, item

200); the memory structure being read-only memory (Arnold: col 4, lines 14-17); and retrieving the client private key from the client's memory (Arnold: col 2, lines 25-41).

Arnold, Aoki, Epstein, and Rose do not explicitly disclose retrieving client authentication data; encrypting the client authentication data with the embedded client private key; and storing the encrypted client authentication data in the client message. However, these limitations are disclosed by Sandhu (paragraph 28).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify the combination invention of Arnold, Aoki, Epstein, and Rose according to the limitations recited in claims 11 and 17 in light of Sandhu's teachings. One skilled would have been motivated to do so because it would provide client-side authentication (Sandhu: paragraph 28), thus making communication between the client and server more secure. Note that Arnold discusses authentication being desired objective for secure communication since before the time of his invention (col 2, lines 43-48).

Claims 12, 18, 25-26, and 29-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (US 5,787,172) in view of Aoki (US 6,745,530) in further view of Epstein et al (US 6,694,025) in further view of Rose (US 5,708,709) in further view of Sandhu et al (US 2002,0078344 and in further view of Davis (US 5,970,147).

Claims 12 and 18:

As per claims 12 and 18, Arnold, Aoki, Epstein, Rose and Sandhu do not explicitly disclose retrieving an embedded client serial number from a read-only memory structure in an article of manufacture in the client; and storing a copy of the embedded client serial number in

the client message. However, these limitations are disclosed by Davis (col 4, lines 26-39; col 5, lines 58-62; and col 6, lines 27-29).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify the combination invention of Arnold, Aoki, Epstein, Rose, and Sandhu according to the limitations recited in claims 12 and 18. One skilled would have been motivated to do so because the client sending the serial number to the server alone with its message would allow the server to index various clients' public keys to the client's serial number, thus providing for a way for the server to look up the client key needed to authenticate the client's message.

Claims 25 and 29:

As per claims 25 and 29, the limitations recited therein are directed towards the server receiving and processing the message sent using the method and computer program product of claims 12 and 18 respectively. One skilled would appreciate that a message sent by a client according to the limitations recited in claims 12 and 18 would be processed by the server according to the limitations recited in claims 25 and 29, thus the rejections for claims 25 and 29 flow from the rejections of claims 12 and 18 respectively.

Claims 26 and 30:

As per claims 26 and 30, the limitations recited therein are directed towards the server processing the authentication data sent by the client using the method, apparatus, and computer program product of claims 11 and 17 respectively. One skilled would appreciate that a message sent by a client according to the limitations recited in claims 11 and 17 would be

processed by the server according to the limitations recited in claims 26 and 30, thus the rejections for claims 26 and 30 flow from the rejections of claims 11 and 17 respectively.

Claims 19, 23, 31 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (US 5,787,172) in view of Rose (US 5,708,709) in further view of official notice by the examiner in further view of Aoki (US 6,745,530) and in further view of Epstein et al (US 6,694,025).

Claims 19 and 23:

As per claim 19, Arnold discloses the following limitations were will known in the art at the time applicant's invention was made:

1. Generating a server message at the server (col 2, lines 9-24).
2. Retrieving a client's public key (col 2, lines 9-24).
3. Encrypting the server message with the client's public key (col 2, lines 9-24).
4. Sending the server message to the client (col 2, lines 9-24).

Note that the cited portion of Arnold discloses communication between two elements A and B. One skilled should appreciate that both A and B can be either a client and/or server.

Arnold does not explicitly disclose that the prior art he discusses teach the following limitations:

1. The server message including application code having a first portion encrypted with a server private key and a second portion, the first portion being authenticable with a server public key.
2. Retrieving information that was requested by the client.

3. Storing the retrieved information in the server message.
4. Wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is generated and stored exclusively outside the client.

However, Rose discloses receiving a server message, the server message including application code having a first portion encrypted with a server private key and a second portion (Fig 4; col 3, lines 50-53; and col 5, lines 44-47), the first portion being authenticable with a server public key (col 8, lines 15-31 and col 10, lines 4-29). Figure 4 shows the format of an application code that is transmitted to the client in response to the client's request for the code. As seen in the Figure, the application code is composed of several portions. The first portion, item 182, is encrypted using the server's private key and the rest is considered the claimed second portion.

Further, note that Arnold also discloses read-only memory being used to store keys (col 4, lines 14-17). At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify the prior art teachings disclosed by Arnold so that the memory structure used to store keys was read-only memory structure. One skilled would have been motivated to do so for the same reasons given in the rejection of claims 10 and 16.

Further, the examiner take official notice that retrieving information that was requested by the client and storing the retrieved information in the server message was well known in the art at the time applicant's invention was made. Note that these limitations were also discussed as being well known in the art at the time applicant's invention was made in a prior office action.

Further, Aoki disclose wherein the client public key corresponds to an embedded client private key in a memory structure in an article of manufacture in the client, and the client public key is stored exclusively outside the client (Fig 1, item 200).

Further, Epstein discloses that it was well known in the prior art to generate public/private key pairs exclusively outside the client, i.e. via a key generation server (col 2, lines 31-39; col 3, line 62-col 4, line 3; and col 4, lines 11-24).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to combine the above teachings to arrive at an invention as recited in claims 19 and 23. One skilled would have been motivated to combine Arnold, Rose, Aoki, Epstein's teachings for the same reasons discussed in the rejection of claims 10 and 16. One skilled would have been motivated to incorporate the teachings the examiner took official notice on because these teachings describe typical client-server relationship, i.e. a client requests information being "served" by the server, the server retrieves the requested information, and sends it to the client via a server message provided that the client is authorized to receive the information.

Claims 31 and 37:

As per claims 31 and 37, the limitations recited therein are directed towards the client receiving and processing the message sent by the server using the method and computer program product of claims 19 and 23 respectively. One skilled would appreciate that a response message sent by a server according to the limitations recited in claims 19 and 23 would be processed by the client according to the limitations recited in claims 31 and 37, thus the rejections for claims 31 and 37 flow from the rejections of claims 19 and 23 respectively.

Claims 20, 24, 32-33, and 38-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (US 5,787,172) in view of Rose (US 5,708,709) in further view of official notice by the examiner in further view of Aoki (US 6,745,530) in further view of Epstein et al (US 6,694,025) and in further view of Sandhu et al (US 2002,0078344).

Claims 20 and 24:

As per claims 20, 22, and 24, Arnold discloses retrieving a server private key (Arnold: col 2, lines 25-41).

Arnold does not explicitly disclose retrieving server authentication data; encrypting the server authentication data with the server private key; and storing the encrypted server authentication data in the server message. However, these limitations are disclosed by Sandhu (paragraph 27).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Arnold's combination invention according to the limitations recited in claims 20 and 24. One skilled would have been motivated to do so because it would provide server-side authentication (paragraph 27), which would make communication between the client and server more secure.

Claims 32 and 38:

As per claims 32 and 38, the limitations recited therein are directed towards the client receiving and processing the message sent by the server using the method, apparatus, and computer program product of claims 20 and 24 respectively. One skilled would appreciate that a response message sent by a server according to the limitations recited in claims 20 and 24

would be processed by the client according to the limitations recited in claims 32 and 38, thus the rejections for claims 32 and 38 flow from the rejections of claims 20 and 24 respectively.

Claims 33 and 39:

As per claims 33 and 39, Arnold does not explicitly disclose retrieving requested information form the server message; and in response to a determination that the decrypted authentication data was verified, processing the requested data. However, the examiner take official notice that the limitations were well known in the art at the time applicant's invention was made. Note that these limitations were also discussed as being well known in the art at the time applicant's invention was made in a prior office action. These limitations describe a typical client-sever relationship. A client typically requests information from a server, the server receives the request, and if the client is authorized to receive the information the server sends the information to the client who receives the requested information via the server's reply message. The client typically only processes the information sent by the server if the decrypted authentication data was verified for security purposes.

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Arnold's invention according to the limitations recited in claims 33 and 39. One skilled would have been motivated to do so because the limitations further recited in claims 33 and 39 describe a typical client-server relationship.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PONNOREAY PICH whose telephone number is (571)272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ponnoreay Pich/
Examiner, Art Unit 2135

/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135